UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/470,054	12/22/1999	SUNIL K. SRIVASTAVA	50325-083	5708

29989 7590 01/16/2004

HICKMAN PALERMO TRUONG & BECKER, LLP
1600 WILLOW STREET
SAN JOSE, CA 95125

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/470,054	SRIVASTAVA ET AL.	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *6*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-13 have been examined.

Claim Objections

2. Claim 1 is objected to because of the following informality: after "node;" in line 19, insert --and--. Appropriate correction is required.

3. Claim 7 is objected to because of the following informality: after "node;" in line 24, insert --and--. Appropriate correction is required.

4. Claim 11 is objected to because of the following informality: replace "node;" in line 10, and replace with --nodes--. Appropriate correction is required.

5. Claim 13 is objected to because of the following informality: after "node;" in line 21, insert --and--. Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the new group session key private key" in line 18. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting the first "the" in line 18 and replacing with --a--.

8. Claims 8-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 8 recites the limitation "one of the leaf nodes" in line 16. There is insufficient antecedent basis for this limitation in the claim.

9. Claims 8-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 8 recites the limitation "the tree structure" in line 8. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "the" in line 8 and replacing with --a--.

10. Claims 8-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 8 recites the limitation "the node" in line 17. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting the first "the" in line 17 and replacing with --a--.

Double Patenting

11. Claim 6 is objected to under 37 CFR 1.75 as being an exact duplicate of claim 5. When two claims in an application are duplicates or else are so close in content that they both cover the

same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

12. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

13. Claims 1, 7, and 13 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 5 of copending Application No. 09/407,785 in view of Dondeti et al., U.S. Patent No. 6,263,435 B1.

As per claims 1, 7, and 13, claim 5 of copending Application No. 09/407,785 incorporates a method comprising:

creating and storing a group session key associated with the multicast group in a directory (see claim 5, lines 2-3; creating and storing a group session key in a directory);

authenticating a first multicast proxy service node with a subset of the multicast proxy service nodes, where each of the multicast proxy service nodes of the multicast group is capable of establishing multicast communication and serving as a key distribution center (see claim 1, lines 3-4) and that are affected by an addition of the first multicast proxy service node to the

multicast group (see claim 1, lines 11-12), based on the group session key stored in the directory (see claim 1, line 12);

receiving a plurality of private keys from the subset nodes (see claim 1, line 13);

receiving a new group session key for the multicast group (see claim 5, lines 3-4; obtaining the group session key), for use after addition of the first multicast proxy service node from a local multicast proxy service node that has received the group session key through periodic replication of the directory (see claim 5, lines 1-5; from a local event service node that is a replica of the first event service node of one domain of the directory);

communicating a new group session key private key to the first multicast proxy service node (see claim 1, lines 15-16; communicating a new private key to the first event service node); and

communicating a message to the subset of nodes that causes the subset of nodes to update their private keys (see claim 1, lines 17-18).

However, claim 5 also includes:

where each event service node is logically organized in a binary tree having a root node, intermediate nodes, and leaf nodes.

Dondeti et al. illustrates a tree structure (see column 3, lines 48-57 and figure 2, items10, 12, and 18). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine this feature with the elements of claims 1, 7, and 13 for managing membership in the multicast group and access to multicast data (see column 3, lines 54-57).

Claim 7 is not patentably distinct from claim 5 of copending Application No. 09/407,785 because the method of claim 5 cannot be practiced by another materially different communication system or by hand from that in claim 7 and the communication system in claim 7 cannot be used to practice another materially different method in claim 5. See MPEP § 806.05(e).

Claim 13 is not patentably distinct from claim 5 of copending Application No. 09/407,785 because the method of claim 5 cannot be practiced by another materially different system of processors instructed by the computer readable medium or by hand from that in claim 13 and the system of processors instructed by the computer readable medium in claim 13 cannot be used to practice another materially different method in claim 5. See MPEP § 806.05(e).

This is a provisional obviousness-type double patenting rejection.

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

15. Claims 1-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Dondeti et al., U.S. Patent No. 6,263,435 B1.

As per claims 1, 7, and 13, Dondeti et al. disclose a method, a communication system, and a computer readable medium for communicating a session key comprising:

creating and storing a group session key associated with the multicast group in a directory (see column 2, lines 62-65; a local subgroup key (LS) used to distribute encrypted data to corresponding subgroup members; see column 4, lines 20-22; figure 2, items 14 and 20; generating a secret key retrievable from a directory and sharing it with all corresponding subgroup members; see column 5, lines 51-54; replacing the subgroup key with a newly created subgroup key retrievable from a directory; see column 6, lines 56-57; generating a data encryption key (DEK));

authenticating a first multicast proxy service node with a subset of multicast proxy service nodes of a multicast group in a communication network, each of which is capable of establishing multicast communication and serving as a key distribution center (see column 3, lines 62-67; column 4, lines 1-3; figure 2, items 10, 14, and 20; a child node in a key group in turn had children in key group; see column 4, lines 14-19; where the child node serves as subgroup manager (SGM) of the key group containing its children) and which are affected by an addition of the first multicast proxy service node to the multicast group, based on the group session key stored in the directory (see column 4, lines 58-66; figure 4, step (101) and item 50; a

host is authenticated by a subgroup manager that can handle additional work load of another member in its subgroup of nodes upon verification of its capability certificate);

receiving a plurality of private keys from the subset of nodes (see column 5, lines 44-48; figure 4, item 60 and step (104); sending the key encrypting key of one of the nodes; see column 7, lines 4-12 and 17-19; figure 2, items p_1, g_2, and h_5; all members of a subgroup have access to the key encrypting keys of the various levels, KEK_1 and KEK_2);

receiving a new group session key for the multicast group, for use after addition of the first multicast proxy service node, from a local multicast proxy service node that has received the group session key through periodic replication of the directory (see column 5, lines 49-55; figure 4, item 70 and step (106); upon adding the new host to its subgroup members' list effectively replicating the members' list of the sender, a local node acting as a subgroup manager SGM changes the subgroup key LS and sends it; see column 7, lines 4-19; where the subgroup members have a replicated directory of key encrypting keys, KEK_1 and KEK_2 used to encrypt a data encrypting key DEK);

communicating the new group session key private key to the first multicast proxy service node (see column 6, lines 62-65; sending the data encryption key for the group, DEK); and

communicating a message to the subset of nodes that causes the subset of nodes to update their private keys (see column 6, lines 31-34; sending a message to all the members which hold a key encrypting key KEK, to request a new key encrypting key KEK).

As per claim 2, Dondeti et al. further point out:

authenticating the plurality of multicast proxy service nodes based on a directory that comprises a directory system agent (DSA) that communicates with one or more of the multicast prosy service nodes (see column 5, lines 51-61; figure 4, step (107); the subgroup manager uses its subgroup members' list to check the existing members before multicasting the new subgroup member key to all subgroup members), and

a replication service agent (RSA) that replicates attribute information of the one or more multicast proxy service nodes (see column 5, lines 19-25; figure 3; and figure 4, item 56; after the new host becomes a subgroup member, the sender generates a message with an authorization certificate containing the new host's identity (H_1) as an attribute).

As per claim 3, Dondeti et al. additionally discuss:

receiving the new group session key from a node of a directory that comprises a directory system agent (DAS) for communicating with one or more of the multicast proxy service nodes (see column 5, lines 49-61; figure 4, item 70 and steps (106) and (107); upon adding the new host to its subgroup members' list, a local node acting as a subgroup manager SGM changes the subgroup key LS and sends it to the new host and to all subgroup members), and

a replication service agent (RSA) for replicating key information of the one or more multicast proxy service nodes (see column 6, lines 25-40; upon a new member subgroup manager SGM, the sender changes the key encrypting key KEK and sends copies of it to the multicast group).

As per claim 4, Dondeti et al. then elaborate:

signaling the replication service agent to carry out replication by storing an updated group session key in a local node of the directory (see column 6, lines 28-44; upon notification that the participant subgroup manager SGM is in the membership database, the sender updates the key encrypting key which is copied for the members and stores it in the updated membership database).

As per claims 5 and 6, Dondeti et al. also describe:

distributing a group session key to all nodes by creating and storing the group session key using a first multicast proxy service node of one domain of the directory (see column 6, lines 56-57; generating a data encryption key (DEK) stored by the sender; column 7, lines 4-9; figure 2, items 1, 10, 12, and 14; distributing the data encryption key (DEK) using the sender's child node of the top level subgroup domain);

replicating the directory (see column 5, lines 49-52; adding the new host to its subgroup member's list effectively replicating the list of the sender); and

obtaining the group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node (see column 7, lines 11-12; figure 2, items 14 and 20; P_1 multicasts the data encryption key (DEK) to g_2 and h_2; see column 4, lines 60-67; figure 4, item 50; where a joined node has equivalent capabilities of other member nodes because of a verified capability certificate).

As per claim 8, Dondeti et al. depict a method for creating a secure multicast or broadcast group comprising:

authenticating the plurality of multicast proxy service nodes via a directory that includes a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes (see column 5, lines 8-15; figure 4, items 50, 52, and 54; the sender uses the capability certificate along with the subgroup manager's identity and the keygroup identity to decide whether a host is a member of the multicast group) and for replicating attribute information of the one or more multicast proxy service nodes (see column 5, lines 19-25; figure 3; and figure 4, item 56; after the new host becomes a subgroup member, the sender generates a message with an authorization certificate containing the new host's identity (H_1) as an attribute);

generating private keys for each of the multicast proxy service nodes, providing unique identification within a tree structure (see column 2, lines 65-67; column 3, lines 1-6; top level key encrypting keys (KEK) accessible to members in a tree structure rooted at the same child of the sender; see column 3, lines 6-8; figure 2, items 12, 14, and h_2; where the number of key groups is limited by the number of SGMs suggesting a unique key for the only child, h_2, of a participant subgroup manager only child, p_1, of a sender, S; column 5, lines 41-46; figure 4, item 64; each host joined has a unique private key);

generating a first group session key for establishing the secure multicast or broadcast group among the multicast proxy service nodes (see column 6, lines 55-57; generating a data encryption key (DEK) to be used in a conventional encryption algorithm);

distributing the first group session key among the multicast proxy service nodes by using periodic directory replication of the attribute information, where the attribute information comprises the first group session key, and the private keys (see column 7, lines 4-9; generating a key distribution packet consisting of the data encryption key (DEK) encrypted by the key

encrypting key (KEK) of the particular subgroup and encrypted by the subgroup key of the top level subgroup (LS_S); see column 7, lines 14-19; where the KEK and LS_S are accessible to the authorized members; see column 8, lines 16-20; through a periodically refreshed directory of keys; see column 5, lines 59-61; figure 4, step (107); periodically replicated to the authorized members); and

forming a second secure multicast group among the plurality of client nodes by a leaf node using a second group session key obtained from a local replica of the node that generated the first group session key (see column 7, lines 4-9; see figure 2, item 22; the key distribution packet that the sender generates is received by each of the sender's children, which decrypts its part of the key distribution packet and reencrypts its decrypted part with the subgroup key that it manages and multicasts the reencrypted part to its children in a subgroup).

As per claim 9, Dondeti et al. further point out:

detecting whether one of the nodes is leaving the secure multicast or broadcast group (see column 7, lines 34-39; determining whether a membership should expire because of expiration of the capability certificate or misbehavior);

determining which of the other nodes are affected by deletion of the leaving node (see column 7, lines 40-45; finding the other subgroup children and sending them a new subgroup key encrypted with encrypted with the public key of each child);

updating the private keys of the affected intermediate nodes using the DSA (see column 6, lines 26-40; the sender updating the key encrypting keys (KEK) of each member of the multicast group when a member leaves to become a participant subgroup manager SGM);

generating a new group session key (see column 7, lines 40-42; changing the local subgroup key);

modifying the attribute information based upon the updated private keys and the new group session key (see column 6, lines 34-37; the sender constructing a list of members authorized to receive the updated key encrypting key (KEK) based on their authorization certificates; see column 7, lines 40-44; where the members are also authorized to receive the new subgroup key); and

distributing the modified attribute information using directory replication (see column 5, lines 49-52; the leaving member-turned participant subgroup manager SGM then obtains its subgroup members' list resembling that of the sender).

As per claim 10, Dondeti et al. additionally elaborate:

receiving a request message from a new node to join the secure multicast or broadcast group (see column 4, lines 58-60; figure 4, step (101); sending a message to join a multicast group that is received by a subgroup manager SGM);

determining which other nodes are affected by addition of the joining node (see column 5, lines 59-61; locating the all the other subgroup members of the subgroup that the node has joined);

updating the private keys of the affected nodes via the DSA (see column 8, lines 25-28; the sender refreshing the key encrypting keys (KEKs) when the node is rejoining as a former member);

generating a new group session key and a private key of the new node (see column 5, lines 30-31; figure 4, item 60; sending the top level key encrypting key KEK as the private key to the joining host; see column 5, lines 52-54; figure 4, item 70; sending the changed subgroup key as a group session key to the new host);

modifying the attribute information based upon the updated private keys, the new group session key, and the private key of the new node (see column 5, lines 51-52; the subgroup manager SGM adding the new host to the subgroup members' list representative of the new subgroup key and the key encrypting keys KEKs of the members); and

distributing the modified attribute information using directory replication (see column 5, lines 41-42; the sender updating the membership database with authorization certificates containing the same attributes as that in the list of the subgroup manager; see column 5, lines 23-25; where the attributes include the member host identity, the corresponding subgroup manager's identity, related to the new subgroup key, and the keygroup identity, related to the key encrypting key KEK).

As per claim 11, Dondeti et al. embody a communication system for creating a secure multicast or broadcast group, comprising:

a plurality of multicast proxy service nodes, each of the multicast proxy service nodes having attribute information comprising a group identification value for uniquely identifying a particular one of the multicast service nodes (see column 5, lines 22-25; figure 3; an authorization certificate containing the host identity, the subgroup manager's SGM's identity, and the keygroup identity), where the plurality of multicast proxy service nodes form a logical

arrangement of the multicast proxy service nodes according to a tree structure, having a root node, intermediate nodes, and leaf nodes (see column 3, lines 48-65; figure 2, items 12, 14, and h_2; where the top node 12 is the sender node, the child node is 14, which itself has a child node, h_2), one of the multicast proxy service nodes being designated as a primary multicast proxy service node mapped to the root node (see column 4, lines 14-19; figure 2, items 1, 10, 12, and 14; where the non-leaf node 14 acts as a subgroup manager and is connected to the top node 12), the other multicast proxy service nodes having private keys corresponding to the group identification values and being mapped to the intermediate nodes and the leaf nodes (see column 4, lines 10-11; figure 2, items h_i; where the end-host members, h_i, are leaf nodes; see column 4, lines 31-33; where there is key encrypting key KEK for members of a key group; see column 5, lines 22-25; figure 3; designated by a key group identity);

a directory comprising a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes to authenticate each of the multicast proxy service nodes (see column 5, lines 8-15; figure 4, items 50, 52, and 54; a sender deciding whether a new node is an authorized member of the multicast group after receiving a message from the node with a membership database) and for replicating the attribute information of the one or more multicast proxy service nodes (see column 5, lines 51-52; figure 2, items 12 and 18; where the subgroup manager SGM 18 has a subgroup members' list with identities related to the nodes like that of the sender 12); and

a plurality of client nodes coupled to one of the multicast proxy service nodes, which creates a secure multicast or broadcast client group that is separate from the secure multicast or broadcast group (see column 4, lines 32-36; figure 2, items 1, 10, and 14; where the nodes inside

key group 1 with a subgroup manager SGM 14, have a distinct key encrypting key from that of key group 10);

in which one of the multicast proxy service nodes generates a first group generates a first group session key for establishing the secure multicast or broadcast group among the plurality of multicast proxy service nodes and distributes the first group session key to other nodes in the group using directory replication (see column 6, lines 55-57; the sender generates a data encryption key (DEK) to be used in a conventional encryption algorithm; see column 7, lines 4-15; the sender distributes the data encryption key (DEK) through each of its children using the local subgroup key that each child manages to the respective subgroup members; see column 5, lines 51-52; in accordance with the subgroup members' list; see column 5, lines 41-42; replicated from the sender's membership database).

As per claim 12, Dondeti et al. delineate a computer system for establishing a secure multicast or broadcast group, comprising:

a communication interface for communicating with a plurality of external computer systems (see column 3, lines 47-57; figure 2; a tree structure communication route connecting; see column 2, lines 46-54; members that are host computer systems) and for interfacing a directory to authenticate the computer system and the plurality of external computer systems (see column 5, lines 41-42; with a membership database containing authorization certificates of the members);

a bus coupled to the communication interface for transferring data (see column 7, lines 4-15; the communication route utilized for the distribution of the data encryption key (DEK)

packet such that the packet bypasses intermediate subgroup managers, without access to the key encrypting key (KEK), to decrypt the data encryption key (DEK), eventually received and decrypted by the end-hosts, with the corresponding the key encrypting key (KEK) to decrypt a portion of the packet to obtain the data encryption key (DEK));

one or more processors coupled to the bus for selectively generating a group session key (see column 5, lines 52-54; changing a subgroup key) and private keys corresponding to the plurality of external computer systems (see column 6, lines 37-39; changing the key encrypting key (KEK) for all the members in the subgroup list), and for logically operating with the plurality of external computer systems according to a tree structure, having a root node, intermediate nodes, and leaf nodes (see column 3, lines 48-65; figure 2, items 12, 14, and h_2; where the top node 12 is the sender node, the child node is 14, which itself has a child node, h_2), wherein the computer system is mapped to the root node (see column 4, lines 14-19; figure 2, items 1, 10, 12, and 14; where the non-leaf node 14 acts as a subgroup manager and is connected to the top node 12), the plurality of external computer systems are mapped to the intermediate nodes and the leaf nodes (see column 4, lines 9-11; figure 2, items h_i; where the end-host members, h_i, are leaf nodes connected to non-leaf nodes); the corresponding private keys providing unique identification of respective plurality of external computer systems within the tree structure (see column 5, lines 22-29; figure 3; an authorization certificate for a host including the key group identity), the group session key being distributed using directory replication using a directory system agent of the directory (see column 5, lines 51-61; the subgroup manager multicasts its new subgroup key to all its subgroup members according to its subgroup members' list; see column 5, lines 41-42; like the sender's membership database); and

a memory coupled to one or more processors via the bus, including one or more sequences of instructions which when executed by the one or more processors cause the one or more processors to perform the step of selectively updating the group session key and the private keys in response to whether a new client joins (see column 8, lines 25-28; the sender refreshing the key encrypting keys (KEKs) when the node is rejoining as a former member; see column 5, lines 30-31; figure 4, item 60; sending the top level key encrypting key KEK as the private key to the joining host; see column 5, lines 52-54; figure 4, item 70; sending the changed subgroup key as a group session key to the new host) or one of the client nodes leaves the multicast or broadcast group (see column 6, lines 26-40; the sender updating the key encrypting keys (KEK) of each member of the multicast group when a member leaves to become a participant subgroup manager SGM; see column 7, lines 40-42; and changing the local subgroup key).

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Thakkar et al., U.S. Patent No. 6,256,733 B1, disclose secure group communication with on-demand availability of stored security credentials of current members.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872 and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (703) 305-1830.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

January 12, 2004

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100